

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 11-205310

(43)Date of publication of application : 30.07.1999

(51)Int.Cl.

H04L 9/36

H04L 9/14

H04L 12/40

(21)Application number : 10-307358

(71)Applicant : MATSUSHITA ELECTRIC IND CO LTD

(22)Date of filing : 28.10.1998

(72)Inventor : IIZUKA HIROYUKI
YAMADA MASAZUMI
TAKECHI HIDEAKI
MATSUZAKI NATSUME

(30)Priority

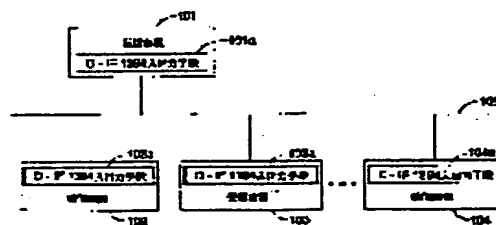
Priority number : 09297614 Priority date : 29.10.1997 Priority country : JP

(54) DATA TRANSMISSION METHOD, DATA RECEPTION METHOD, DATA TRANSMISSION SYSTEM AND PROGRAM RECORDING MEDIUM

(57)Abstract:

PROBLEM TO BE SOLVED: To further surely protect transmission data by deciding the kind of ciphering to be applied corresponding to the management information of data, enciphering the data and transmitting them together with management information.

SOLUTION: The mode decision means of a transmitter 101 decides the group of a cryptographic key to be used corresponding to the contents of the copy management information of video data or the like to be transmitted and outputs it to a key generation means as cipher mode information. The key generation means generates a key to be used for enciphering within the decided group (A or B) of the key, based on it. When information is sent from a mode detection means, the key obtaining means of a receiver 102 sends the transfer request of key information for starting the obtaining of the key to a D-IF1394 input/output means 102a. The key obtaining means sends the key information transferred from the side of the transmitter 101 to a key preservation means and it is temporarily preserved there and outputted to an enciphering means. The deciphering means decipheres actual data by utilizing the key information from the key preservation means and key change information from a packet decoding means.



LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

Copyright (C); 1998,2000 Japan Patent Office

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開平11-205310

(43) 公開日 平成11年(1999) 7月30日

(51) Int.Cl. ⁴	識別記号	F I	
H 0 4 L 9/36		H 0 4 L 9/00	6 8 5
9/14			6 4 1
12/40		11/00	3 2 0

審査請求 未請求 請求項の数31 O L (全 15 頁)

(21) 出願番号	特願平10-307358	(71) 出願人	000005821 松下電器産業株式会社 大阪府門真市大字門真1006番地
(22) 出願日	平成10年(1998)10月28日	(72) 発明者	飯塚 裕之 大阪府門真市大字門真1006番地 松下電器産業株式会社内
(31) 優先権主張番号	特願平9-297614	(72) 発明者	山田 正純 大阪府門真市大字門真1006番地 松下電器産業株式会社内
(32) 優先日	平9(1997)10月29日	(72) 発明者	武知 秀明 大阪府門真市大字門真1006番地 松下電器産業株式会社内
(33) 優先権主張国	日本 (J P)	(74) 代理人	弁理士 松田 正道

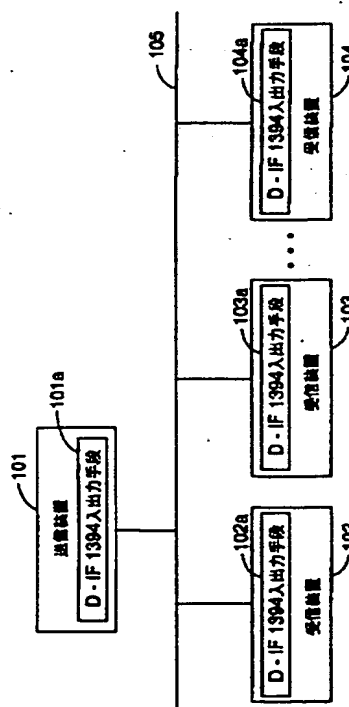
最終頁に続く

(54) 【発明の名称】 データ送信方法、データ受信方法、データ伝送システム、及びプログラム記録媒体

(57) 【要約】

【課題】 コピー管理情報の改竄により復号化された実データが不正記録される。

【解決手段】 送信データの管理情報に応じて送信データに適用する暗号鍵を決定するモード決定手段202と、その決定された鍵により送信データを暗号化する暗号化手段205と、暗号化されたデータとデータ管理情報とを送信する1394入出力手段101aと、送信されてきた送信データを受信する1394入出力手段102aと、その受信データからデータ管理情報を検出するパケット読取手段301と、送信データの送信元に対して、検出したデータ管理情報を送り、且つ、その送信したデータ管理情報に対応する鍵を要求する鍵入手手段302と、鍵の送信要求があった場合、データ管理情報に対応した鍵を要求元に送信する鍵配布手段206と、送信されてきた鍵により受信データを復号化する復号化手段304等を備える。



【特許請求の範囲】

【請求項1】 送信対象となるデータの管理情報に応じて前記データの送信に適用する暗号化の種類を決定し、その決定された暗号化の種類に基づいて、前記データを暗号化し、前記暗号化されたデータと前記データ管理情報とを送信することを特徴とするデータ送信方法。

【請求項2】 請求項1記載のデータ送信方法により送信されてきた送信データを受信し、その受信データから前記データ管理情報を検出し、前記送信データの送信元に対して、前記検出したデータ管理情報を送り、且つ、その送信したデータ管理情報に対応する復号化情報を要求することを特徴とするデータ受信方法。

【請求項3】 請求項2記載のデータ受信方法により前記復号化情報の要求があった場合、前記データ管理情報に対応した前記復号化情報を前記要求元に送信することを特徴とする請求項1記載のデータ送信方法。

【請求項4】 請求項3記載のデータ送信方法により送信されてきた前記復号化情報に基づいて、前記受信データを復号化し、前記検出されたデータ管理情報に応じて、前記復号化した受信データの処理の仕方を決定することを特徴とする請求項2記載のデータ受信方法。

【請求項5】 前記データ管理情報が同一の場合であっても、前記暗号化の種類を時間と共に更新し、前記送信対象となるデータを前記更新された暗号化の種類により暗号化し、前記暗号化されたデータを送信する以前に、前記更新を行うことを予告する予告情報を送信することを特徴とする請求項1又は3記載のデータ送信方法。

【請求項6】 前記データ管理情報が同一の場合であっても、前記暗号化の種類を時間と共に更新し、前記更新を行ったことを示す情報を送信し、前記データ管理情報に対応する復号化情報の要求があった場合、その時点で使用されるべき復号化情報と、次の時点で使用される予定の復号化情報との双方を送信することを特徴とする請求項1又は3記載のデータ送信方法。

【請求項7】 前記暗号化の種類を時間と共に更新する場合、その更新された前記暗号化の種類が、前記データ管理情報に応じて決定された前記他の暗号化の種類と重複しないことを特徴とする請求項5又は6記載のデータ送信方法。

【請求項8】 請求項5記載のデータ送信方法により送信されてきた前記予告情報を受信した場合、その予告情報に応じて、前記送信データの送信元に対して前記復号化情報を要求することを特徴とする請求項2又は4記載のデータ受信方法。

【請求項9】 請求項6に記載のデータ送信方法により

送信されてきた前記更新を行ったことを示す情報を受信した場合、その受信した情報に基づいて、前記情報の送信元に対して、前記復号化情報を要求することを特徴とする請求項2又は4記載のデータ受信方法。

【請求項10】 前記データ管理情報を送るとは、前記検出したデータ管理情報をそのまま送る、又は、前記検出したデータ管理情報を所定の変換を行って送ることであることを特徴とする請求項2又は8記載のデータ受信方法。

【請求項11】 前記データ管理情報に応じて前記データの送信に適用する暗号化の種類を決定するとは、前記データ管理情報に応じて暗号化に用いる鍵を異ならせることであることを特徴とする請求項1又は3記載のデータ送信方法。

【請求項12】 前記データ管理情報に応じて前記データの送信に適用する暗号化の種類を決定するとは、前記データ管理情報に応じて暗号化に用いるアルゴリズムを異ならせることであることを特徴とする請求項1又は3記載のデータ送信方法。

【請求項13】 前記データ管理情報とは、前記データがコピー自由であるのか、1回コピー可能であるのか、又はコピー禁止であるのかを示す情報を含むコピー管理情報であることを特徴とする請求項1、3、5又は6記載のデータ送信方法。

【請求項14】 前記コピー禁止であることを示す情報には、元からコピー禁止であることを示す情報と、元々1回コピー可能であったが、その1回のコピーが実行されたためにその後のコピーが禁止となったことを意味する更なるコピー禁止を示す情報との2種類の情報が含まれており、

前記暗号化の種類は、それら2種類の情報に応じて異なることを特徴とする請求項13記載のデータ送信方法。

【請求項15】 請求項13記載のデータ送信方法により送信されてきたデータ管理情報が、1回コピー可能であることを示している場合、前記1回コピー可能であることを示す情報をデータ管理情報として有するデータを所定の記録媒体に記録する際、そのデータ管理情報を前記1回コピー可能からコピー禁止を示す内容に変更し、そのコピー禁止を示すデータ管理情報と共に前記記録を行うことを特徴とする請求項8又は9に記載のデータ受信方法。

【請求項16】 請求項14記載のデータ送信方法により送信されてきたデータ管理情報が、1回コピー可能であることを示している場合、前記1回コピー可能であることを示す情報をデータ管理情報として有するデータを所定の記録媒体に記録する際、そのデータ管理情報を前記1回コピー可能から前記更なるコピー禁止を示す内容に変更し、その更なるコピー禁止を示すデータ管理情報と共に前記記録を行うことを特徴とする請求項8又は9に記載のデータ受信方法。

【請求項17】 送信対象となるデータの管理情報に応じて前記データの送信に適用する暗号化の種類を決定するモード決定手段と、

その決定された暗号化の種類に基づいて、前記データを暗号化する暗号化手段と、

前記暗号化されたデータと前記データ管理情報とを送信するデータ送信手段と、

前記データ送信手段により送信されてきた送信データを受信するデータ受信手段と、

その受信データから前記データ管理情報を検出するデータ管理情報検出手段と、

前記送信データの送信元に対して、前記検出したデータ管理情報を送り、且つ、その送信したデータ管理情報に対応する復号化情報を要求する復号化情報要求手段と、

前記復号化情報の要求があった場合、前記データ管理情報に対応した前記復号化情報を前記要求元に送信する復号化情報送信手段と、

前記送信されてきた前記復号化情報に基づいて、前記受信データを復号化する復号化手段と、

前記検出されたデータ管理情報に応じて、前記復号化された受信データの処理の仕方を決定する処理方法決定手段と、を備えたことを特徴とするデータ伝送システム。

【請求項18】 前記データ管理情報を送るとは、前記検出したデータ管理情報をそのまま送る、又は、前記検出したデータ管理情報を所定の変換を行って送ることであることを特徴とする請求項17記載のデータ伝送システム。

【請求項19】 前記データ管理情報に応じて前記データの送信に適用する暗号化の種類を決定するとは、前記データ管理情報に応じて暗号化に用いる鍵を異ならせることであることを特徴とする請求項17記載のデータ伝送システム。

【請求項20】 前記データ管理情報に応じて前記データの送信に適用する暗号化の種類を決定するとは、前記データ管理情報に応じて暗号化に用いるアルゴリズムを異ならせることであることを特徴とする請求項17記載のデータ伝送システム。

【請求項21】 前記データ管理情報が同一の場合であっても、前記暗号化の種類を時間と共に更新する暗号化種類更新手段と、

前記更新を行うことを予告するための予告情報を生成する予告情報生成手段とを備え、

前記暗号化手段が前記送信対象となるデータを前記暗号化する場合、前記更新された暗号化の種類により暗号化し、

前記生成された予告情報が、前記更新された暗号化の種類により暗号化されたデータを送信する以前に送信されることを特徴とする請求項17記載のデータ伝送システム。

【請求項22】 前記データ管理情報が同一の場合であ

っても、前記暗号化の種類を時間と共に更新する暗号化種類更新手段と、

前記更新を行ったことを通知するための更新情報を生成する更新実行情報生成手段とを備え、

前記暗号化手段が前記送信対象となるデータを前記暗号化する場合、前記更新された暗号化の種類により暗号化し、

前記更新された暗号化の種類により暗号化されたデータの送信が開始される際に、前記更新情報が送信されることを特徴とする請求項17記載のデータ伝送システム。

【請求項23】 前記復号化情報要求手段は、受信された前記予告情報に応じて、前記送信データの送信元に対して前記復号化情報を要求することを特徴とする請求項21のデータ伝送システム。

【請求項24】 前記復号化情報要求手段は、受信された前記更新情報の変化に応じて、前記送信データの送信元に対して、前記復号化情報を要求することを特徴とする請求項22記載のデータ伝送システム。

【請求項25】 前記暗号化の種類を時間と共に更新する場合、その更新された前記暗号化の種類が、前記データ管理情報に応じて決定された前記他の暗号化の種類と重複しないことを特徴とする請求項21～24の何れか一つに記載のデータ伝送システム。

【請求項26】 前記データ管理情報とは、前記データがコピー自由であるのか、1回コピー可能であるのか、又はコピー禁止であるのかを示す情報を含むコピー管理情報であることを特徴とする請求項17～25の何れか一つに記載のデータ伝送システム。

【請求項27】 前記コピー禁止であることを示す情報には、元からコピー禁止であることを示す情報と、元々1回コピー可能であったが、その1回のコピーが実行されたためにその後のコピーが禁止となったことを意味する更なるコピー禁止を示す情報との2種類の情報が含まれており、

前記暗号化の種類は、それら2種類の情報に応じて異なることを特徴とする請求項26記載のデータ伝送システム。

【請求項28】 前記データ送信手段により送信されてきたデータ管理情報が、1回コピー可能であることを示している場合、

前記1回コピー可能であることを示す情報をデータ管理情報として有するデータが所定の記録媒体に記録される際、そのデータ管理情報が、前記1回コピー可能からコピー禁止を示す内容に変更されて、そのコピー禁止を示すデータ管理情報と共に前記記録が行われることを特徴とする請求項26に記載のデータ伝送システム。

【請求項29】 前記データ送信手段により送信されてきたデータ管理情報が、1回コピー可能であることを示している場合、

前記1回コピー可能であることを示す情報をデータ管理

情報として有するデータが所定の記録媒体に記録される際、そのデータ管理情報が、前記1回コピー可能から前記更なるコピー禁止を示す内容に変更されて、その更なるコピー禁止を示すデータ管理情報と共に前記記録が行われることを特徴とする請求項27に記載のデータ伝送システム。

【請求項30】請求項1～16の何れか一つに記載の各ステップの全部又は一部のステップをコンピュータに実行させるためのプログラムを記録したことを特徴とするプログラム記録媒体。

【請求項31】請求項17～29の何れか一つの請求項に記載の各手段の全部又は一部の手段の機能をコンピュータに実行させるためのプログラムを記録したことを特徴とするプログラム記録媒体。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、例えば、デジタルデータを送受信する、データ送信方法、データ受信方法、データ伝送システム、及びプログラム記録媒体に関するものである。

【0002】

【従来の技術】従来のデータ転送方式には、IEEE1394規格(IEEE: THE INSTITUTE OF ELECTRICAL AND ELECTRONIC ENGINEERS, INC)を用いたデータ転送方法がある。(参考文献: IEEE1394 High Performance Serial Bus) IEEE1394規格におけるデータ転送には、映像信号や音声信号等の同期データの転送に適したアイソクロノス通信と、制御信号等の非同期データの転送に適したエイシンクロナス通信とがあり、両通信はIEEE1394バス上で混在することが可能である。

【0003】アイソクロノス通信は、いわゆる放送型の通信であり、IEEE1394バス上のある装置が出力するアイソクロノスパケットは、同バス上の全ての装置が受信することができる。

【0004】これに対してエイシンクロナス通信は、1対1の通信と放送型通信の両方がある。そして、バス上のある装置が出力するエイシンクロナスパケットには、そのパケットを受信すべき装置をあらわす識別子が含まれており、その識別子が特定の装置をあらわす時にはその識別子で指定された装置が当該エイシンクロナスパケットを受信し、識別子がブロードキャストをあらわす時には同バス上の全ての装置が当該エイシンクロナスパケットを受信する。

【0005】また、IEEE1394規格を用いてデジタル音声信号やデジタル映像信号等を転送したり、IEEE1394バス上につながれた機器間でデータ伝送経路の接続管理を行うための規格として、IEC(IEC: International Electrotechnical Commission 国際電気標準会議)においてIEC61883規格(以下、AVプロト

コルにおいては、映像音声データはアイソクロノスパケット内に配置されて転送される。また、アイソクロノスパケットはCIPヘッダ(CIP: Common Isochronous Packet)を含む。CIPヘッダ内には映像音声データの種別を示す識別情報や、アイソクロノスパケットを送信している送信装置の装置番号等の情報が含まれている。

【0006】このような従来のデータ転送方式を用いたデータ伝送システムにおいて、送信対象となるデータの著作権保護の観点から、転送対象となるデータの複製の制限をデータ保護情報により行えるデータ伝送システムが提案されている。この様に、複製制限の仕組みが必要なデジタルデータとしては、例えば、映像をデジタル化したビデオデータや、音声をデジタル化したオーディオデータや、あるいは両方を合わせて構成されたデジタルデータなどがある。

【0007】以下に、このような従来のデータ伝送システムについて、図6を参照しながらその構成を述べる。

【0008】即ち、図6は、従来のデータ伝送システムにて使用されるアイソクロノスパケットのフォーマットをあらわす図である。

【0009】同図に示す通り、アイソクロノスパケット101は、アイソクロノスパケットヘッダ900、ヘッダCRC901、アイソクロノスペイロード902、データCRC903からなる。

【0010】アイソクロノスパケットヘッダ900には、データ保護情報を格納するためのSyフィールド910が含まれる。Syフィールド910の上位2ビットに格納された値が00である時には、送信対象となるデータ(後述する実データ905)が、複製が自由に行えるデータである事を示している。また、10である時には、そのデータが、1回のみ複製可能であることを、更に、11である時には、そのデータが、複製禁止であることを示している。

【0011】又、アイソクロノスパケットヘッダ900には2ビットのタグ907が含まれる。タグ907は、その値が01である時には、そのアイソクロノスパケットがAVプロトコルに準拠したアイソクロノスパケットであることを示す。タグ907の値が01であるとき、即ち、そのアイソクロノスパケットがAVプロトコル準拠のアイソクロノスパケットである時には、アイソクロノスペイロード902の先頭にCIPヘッダ904が含まれる。

【0012】CIPヘッダ904の中には、当該アイソクロノスパケットを出力している出力装置の識別子であるソースID906が含まれる。また、CIPヘッダ904には、アイソクロノスペイロード902に含まれる実データ905がどのような種類のデータであるかをあらわすFMT908やFDF909が含まれる。

【0013】映像や音声の送信対象となるデータは実データ905に含まれるが、この実データ905は、上述

したデータ保護情報が、10又は11である場合には、暗号化されたデータであるが、コピーフリーを意味する00の場合には、暗号化はされていない。又、データ保護情報は、実データ905中にも含まれており、一般に、CDの場合はSCMSと、また、DVの場合はCGMS等と呼ばれている。

【0014】このような構成において、次に動作を説明する。すなわち、送信機はデジタルデータを送信する際に、コピーしてよいかどうかの条件を示すデータ保護情報を、アイソクロノスケットヘッダ900のSyフィールド910に格納して、実データ905と共に送信する。受信機側は、受信したデータのSyフィールド910の中からデータ保護情報を検出して、データ保護情報の内容を解釈した結果に基づいて、デジタルデータを記録するときの機器の動作を切り替える。又、コピーフリーのデータである場合を除いて、実データが暗号化されているので、受信機側は、それを復号化するために必要な復号化情報の転送を送信機側へ要求する。送信機は、その要求を受けて、復号化情報をその要求元へ送る。受信機は、送信機から送られてきた復号化情報を用いて、受信した実データ905を復号化する。この様にして復号化された実データ905は、表示装置に表示される。一方、その復号化された実データの記録動作に関しては、データ保護情報の内容に基づいて適宜切り替えられる。

【0015】即ち、受信機が、例えばVTRであるならば、検出したデータ保護情報が、“コピー1回可能”を意味している場合、復号化されたデータがVTRに内蔵されたビデオテープに記録される。又、“コピー禁止”を意味している場合、仮に録画ボタンが押されていたとしても、記録動作は行われない。

【0016】

【発明が解決しようとする課題】しかし、このような従来のデータ伝送システムでは、不正行為を行おうとする者により、送信機側と受信機側の間の伝送路中において、Syフィールド910の中に格納されているデータ保護情報が改竄された場合、復号化されたデータが不正にコピーされてしまうという課題を有していた。

【0017】即ち、例えば、送信機から送信された段階では、アイソクロノスケットヘッダ900のSyフィールド910の中に格納されているデータ保護情報の値が11であり、“コピー禁止”を意味していた場合に、不正行為者が、伝送路において、そのデータ保護情報の値を“コピー1回可能”を意味する10に改竄したとする。以下、この場合について更に具体的に説明する。

【0018】即ち、この場合、受信機側のVTRは、Syフィールド910の中に格納されているデータ保護情報を見て、その値が10であることを検出する。この場合、実データ905は上述した様に暗号化されているので、それを復号化するための復号化情報の送信要求を送

信機に対して送る。この要求を受けた送信機は、要求元の受信機に対して復号化情報を送る。受信機側は、送られてきた復号化情報を用いて、実データ905を復号化した上で、その復号化された実データを表示装置等に表示する。一方、VTRは、上述した通り、Syフィールド910の中に格納されているデータ保護情報の値が10であることを検出しているのので、受信した実データ905が、本来コピー禁止のデータであるにも関わらず、コピー1回可能と判断して、上記復号化された実データをビデオテープに録画してしまうという課題を有していた。

【0019】本発明は、上記従来のデータ伝送システムのこのような課題を考慮し、伝送データの保護が従来に比べてより一層確実にできるデータ送信方法、データ受信方法、データ伝送システム、及びプログラム記録媒体を提供することを目的とする。

【0020】

【課題を解決するための手段】第1の本発明（請求項1記載の発明に対応）は、送信対象となるデータの管理情報に応じて前記データの送信に適用する暗号化の種類を決定し、その決定された暗号化の種類に基づいて、前記データを暗号化し、前記暗号化されたデータと前記データ管理情報とを送信するデータ送信方法である。

【0021】又、第2の本発明（請求項2記載の発明に対応）は、上記第1の本発明のデータ送信方法により送信されてきた送信データを受信し、その受信データから前記データ管理情報を検出し、前記送信データの送信元に対して、前記検出したデータ管理情報を送り、且つ、その送信したデータ管理情報に対応する復号化情報を要求するデータ受信方法である。

【0022】又、第3の本発明（請求項3記載の発明に対応）は、上記第2の本発明のデータ受信方法により前記復号化情報の要求があった場合、前記データ管理情報に対応した前記復号化情報を前記要求元に送信する上記第1の本発明のデータ送信方法である。

【0023】又、第4の本発明（請求項4記載の発明に対応）は、上記第3の本発明のデータ送信方法により送信されてきた前記復号化情報に基づいて、前記受信データを復号化し、前記検出されたデータ管理情報に応じて、前記復号化した受信データの処理の仕方を決定する上記第2の本発明のデータ受信方法である。

【0024】又、第17の本発明（請求項17記載の発明に対応）は、送信対象となるデータの管理情報に応じて前記データの送信に適用する暗号化の種類を決定するモード決定手段と、その決定された暗号化の種類に基づいて、前記データを暗号化する暗号化手段と、前記暗号化されたデータと前記データ管理情報とを送信するデータ送信手段と、前記データ送信手段により送信されてきた送信データを受信するデータ受信手段と、その受信データから前記データ管理情報を検出するデータ管理情報

検出手段と、前記送信データの送信元に対して、前記検出したデータ管理情報を送り、且つ、その送信したデータ管理情報に対応する復号化情報を要求する復号化情報要求手段と、前記復号化情報の要求があった場合、前記データ管理情報に対応した前記復号化情報を前記要求元に送信する復号化情報送信手段と、前記送信されてきた前記復号化情報に基づいて、前記受信データを復号化する復号化手段と、前記検出されたデータ管理情報に応じて、前記復号化された受信データの処理の仕方を決定する処理方法決定手段と、を備えたデータ伝送システムである。

【0025】又、第21の本発明（請求項21記載の発明に対応）は、上記データ管理情報が同一の場合であっても、前記暗号化の種類を時間と共に更新する暗号化種類更新手段と、前記更新を行うことを予告するための予告情報を生成する予告情報生成手段とを備え、前記暗号化手段が前記送信対象となるデータを前記暗号化する場合、前記更新された暗号化の種類により暗号化し、前記生成された予告情報が、前記更新された暗号化の種類により暗号化されたデータを送信する以前に送信される上記第17の本発明のデータ伝送システムである。

【0026】又、第22の本発明（請求項22記載の発明に対応）は、上記データ管理情報が同一の場合であっても、前記暗号化の種類を時間と共に更新する暗号化種類更新手段と、前記更新を行ったことを通知するための更新情報を生成する更新実行情報生成手段とを備え、前記暗号化手段が前記送信対象となるデータを前記暗号化する場合、前記更新された暗号化の種類により暗号化し、前記更新された暗号化の種類により暗号化されたデータの送信が開始される際に、前記更新情報が送信される上記第17の本発明のデータ伝送システムである。

【0027】以上の構成により、本発明は、伝送データの保護が従来に比べてより一層確実に行える。

【0028】

【発明の実施の形態】以下、本発明のデータ伝送システムの一実施の形態について、図面を参照しながら説明する。

【0029】図1は、本実施の形態のデータ伝送システムの全体を示した概略構成図であり、図2、3は、そのデータ伝送システムを構成する送信装置、および受信装置についての構成図である。

【0030】以下、同図を用いて本実施の形態の構成について述べる。

【0031】図1に示す様に、本実施の形態のデータ伝送システムは、送信装置101と、複数の受信装置102～104が、IEEE1394バス105によって接続されている。それぞれの装置101～104と、IEEE1394バス105との接続は、D-IF1394入出力手段（101a～104a）を介して行われている。

【0032】又、送信装置101と、複数の受信装置102～104との間におけるデータ転送は、従来のデータ伝送システムについて説明したものと同様である。即ち、映像信号や音声信号等の同期データの転送に適したアイソクロノス通信と、制御信号等の非同期データの転送に適したエイシンクロナス通信とが、IEEE1394バス105上で混在可能な構成となっている。

【0033】次に、図2を用いて、本実施の形態の送信装置101の内部構成を述べる。

【0034】即ち、図2に示すように、データ出力手段201は、1394バス105上に送信しようとする所定長の映像データ等をモード決定手段202及び暗号化手段205に対して出力する手段である。モード決定手段202は、送信しようとする映像データ等のコピー管理情報の内容に応じて、暗号化の鍵としてどのグループの鍵を用いるかを決定し、その決定された内容を暗号モード情報として鍵発生手段203に出力する手段である。コピー管理情報と暗号化モードとの対応は更に後述する。本実施の形態では、コピー管理情報は、コピーフリー、コピー1回可能、及びコピー禁止の3種類の著作権の保護のレベルを示す情報であるとする。本実施の形態のコピー管理情報は、本発明のデータ管理情報に対応する。また、鍵発生手段203は、モード決定手段202からの暗号モード情報に従って、決定された鍵のグループ（グループA又は、B）内において、暗号化に用いる鍵203aを発生させる手段である。この鍵の発生は、切り替えタイミング決定手段207からの切り替え情報207aに応じて時間的に順次行われるものであり、且つ、発生された鍵は全て異なる。

【0035】ここで、上述した通り、コピー管理情報と暗号化モードとの対応について更に述べる。

【0036】即ち、本実施の形態では、上記3種類のコピー管理情報に対応して、コピーフリーでは、暗号化を行わないものとし、コピー1回可能では暗号鍵はグループAの中から決定され、又、コピー禁止では暗号鍵はグループBの中から決定されるものとする。換言すれば、暗号化モード情報は、暗号鍵のグループを識別する情報である。尚、グループAとグループBとは、共通する鍵を持たないとする。

【0037】又、鍵保存手段204は、鍵発生手段203により発生された鍵203aを一時的に保存し、保存している鍵203aを暗号化手段205に出力する手段である。暗号化手段205は、データ出力手段201から出力されてきた映像データ201aを鍵保存手段204から送られてきた鍵203aを用いて暗号化し、暗号化データ205aをパケット生成手段209に出力する手段である。鍵配布手段206は、受信装置からの要求に応じて、要求元の認証作業及びその認証結果に基づく鍵203aの配布を非同期通信により行い、又、鍵203aの配布の完了した旨を切り替えタイミング決定手

段207に送る手段である。切り替えタイミング決定手段207は、上述した様に、モード決定手段202により決定された鍵のグループ内において、時間とともに暗号化に用いる鍵を更新していくための、鍵の切り替え時期を決定する手段であり、その切り替え時期を示す切り替え情報207aを鍵発生手段203及び変更情報発生手段208に送る手段である。変更情報発生手段208は、鍵配布手段206、切り替えタイミング決定手段207からの情報を得て、イントランジションモード情報を作成する手段であり、モード決定手段202から送られてくるコピー管理情報（暗号モードと対応）とイントランジションモード情報とを選択的にパケット生成手段209へ出力する手段である。

【0038】ここで、イントランジションモード情報とは、同一の暗号モード内において、鍵が切り替えられるタイミングを事前に予告するための情報である。

【0039】又、本実施の形態では、暗号モード情報とイントランジションモード情報は、いずれも図6で述べたアイソクロノスパケットヘッダ900内のSyフィールド910に格納されるもので、2ビットからなるデータ208aである。

【0040】又、この2ビットデータ208aのパターンと、コピー管理情報（暗号モード情報と対応）及びイントランジションモード情報との対応は、次の通りである。

【0041】即ち、コピー管理情報がコピーフリーでは00、コピー1回可能では10、コピー禁止では11とし、イントランジションモードには01を当てはめるものとする。

【0042】パケット生成手段209は、暗号化データ205a（図6の実データ905に対応）と、Syフィールドに格納される2ビットデータ208aとを得て、同期通信によりデータバス105上へ送信されるデータパケット209aを生成し、それをD-IF1394入出力手段101aに出力する手段である。尚、本実施の構成では、データパケットの構成は、図6で述べた構成と基本的に同じである。

【0043】又、D-IF1394入出力手段101aは、1394バス105と送信装置101との間でアイソクロノスパケットおよびエイシンクロナスパケットの入出力を行う。すなわち、パケット生成手段209の出力するデータパケット209a（アイソクロノスパケット）、および鍵配布手段206の出力する鍵情報203a（エイシンクロナスパケット）を1394バス105上に出力するとともに、1394バス105から受信したエイシンクロナスパケットを鍵配布手段206へと出力する手段である。

【0044】次に、図3を用いて、本実施の形態の受信装置102の内部構成を述べる。

【0045】即ち、図3に示す様に、D-IF1394

入出力手段102aは、1394バス105と受信装置102との間でアイソクロノスパケットおよびエイシンクロナスパケットの入出力を行う。すなわち、D-IF1394入出力手段102aは、1394バス105から受信したアイソクロノスパケットのデータパケット209aをパケット解読手段301に対して出力し、1394バス105から受信したエイシンクロナスパケットの鍵情報203aを鍵入手手段302に対して出力する手段である。また、D-IF1394入出力手段102aは、鍵入手手段302の出力する、エイシンクロナスパケットである鍵情報転送要求を1394バス105に対して出力する手段である。

【0046】パケット解読手段301は、D-IF1394入出力手段102aからのデータパケット209aを得て、パケットの内、Syフィールド910（図6参照）から2ビットのデータを抽出し、その2ビットデータの内容を解読して、抽出した2ビットデータをモード検出手段303へ送り、又、それがイントランジションモード（変更情報）を示している場合には、抽出した2ビットデータを復号化手段304へも送る手段である。又、パケット解読手段301は、2ビットデータの内容を解読した結果に応じて、パケットの内の実データ905（図6参照）を復号化手段304、又はデータ記録再生手段305へ送る手段である。

【0047】モード検出手段303は、パケット解読手段301から送られてきたコピー管理情報の内容を調べ、調べた結果に応じて、実データ905の復号用の鍵を入手する必要がある旨の情報を鍵入手手段302へ送る手段である。

【0048】鍵入手手段302は、モード検出手段303から上記情報が送られてきた場合、鍵の入手を開始するための鍵情報の転送要求をD-IF1394入出力手段102aに送る手段である。尚、ここで重要なことは、この転送要求には、モード検出手段303から送られてきたコピー管理情報が添付されていることである。

【0049】尚、このコピー管理情報の添付は、コピー管理情報をそのまま添付しても良いし、何らかの値に変換してから添付しても良い。所定の変換して添付する場合には、送信装置101は変換のルールを知っており、変換前のコピー管理情報を検出することが出来る。所定の変換の例としては、例えば、2ビットの01を4ビットの0100に変換し、10を0010に変換するという変換をして、この4ビットを送る構成が考えられる。

【0050】又、鍵入手手段302は、送信装置101側から転送されてきた鍵情報203aを鍵保存手段306へ送る手段である。尚、本発明のデータ管理情報検出手段は、パケット解読手段301と、モード検出手段303を含むものである。

【0051】鍵保存手段306は、鍵入手手段302から送られてきた鍵情報を一時的に保存し、所定のタイミ

ングで復号化手段304へその鍵情報を出力する手段である。

【0052】復号化手段304は、鍵保存手段306からの鍵情報とパケット解読手段301からの鍵の変更情報310とを利用して、実データ905を復号化する手段である。

【0053】データ記録再生手段305は、復号化手段304で復号化されたAVデータを又は、パケット解読手段301から直接送られてきたAVデータを表示手段307へ送り表示させる手段であり、内蔵する記録媒体に記録する手段である。又、音声出力手段308は、データ記録再生手段305からの音声データを出力する手段である。

【0054】尚、その他の受信装置103~104についても、上記と同様の構成である。

【0055】以上の構成において、次に、本実施の形態の動作を図2~図4を参照しながら述べながら、本発明のデータ送信方法、データ受信方法の一実施の形態についても同時に説明する。

【0056】図4は、本実施の形態のSyフィールド910（図6参照）に格納された2ビットデータ及び暗号鍵の時間的变化を示す図である。

【0057】図4に示すように、本実施の形態では、送信装置101は、時刻T1までは第1のAVデータ401を、時刻T1からT6の間では第2のAVデータ402を、そして、時刻T6からT7の間では音声データ403を、更に、その後は、第3のAVデータ404を1394バス105上に転送しているものとする。

【0058】又、これら転送データのコピー管理情報は、同図に示すとおり、それぞれ、前から順番に、コピー禁止、コピー1回可能、コピーフリー、そしてコピー禁止である。従って、各転送データと、使用する鍵のグループとの対応関係は、同図に示すとおり、第1のAVデータ401、第2のAVデータ402、そして第3のAVデータ404の転送は、それぞれこの順番にグループB、グループA、そしてグループBがそれぞれ対応する。又、音声データ403は、コピーフリーであり、暗号化されないので該当するグループは存在しない。更に又、第2のAVデータ402の転送中に、グループAの中で暗号鍵が3回更新（鍵A1~A3）されるものとする。

【0059】（1）先ず、時刻T1直後における動作を述べる。

【0060】即ち、モード決定手段202（図2参照）は、データ出力手段201から出力されてくる第2のAVデータのコピー管理情報を検出して、コピー1回可能であること判定し、それに対応する暗号鍵のグループをAと決めて、鍵発生手段203に伝える。鍵発生手段203は、グループAにおいて、暗号鍵A1を作成して、鍵保存手段204へ送る。暗号化手段205は、鍵保存

手段204から送られてきた暗号鍵A1を用いて、第2のAVデータ402を暗号化する。パケット生成手段209は、暗号化された第2のAVデータ402を実データ905とし、変更情報発生手段208を介して送られてきたコピー管理情報の「10」をSyフィールド910に格納して、データパケットとしてD-IF1394入出力手段101aに出力する。

【0061】一方、受信装置102（図3参照）では、1394バス105上に転送された第2のAVデータ402を含むデータパケットをD-IF1394入出力手段102aを介して受信する。

【0062】具体的には、パケット解読手段301が、受信されたデータパケットからSyフィールド910に格納されているコピー管理情報である2ビットデータ「10」を抽出し、その内容から実データ905が暗号化されていること判定する。そして、実データ905の復号用の鍵を入手する必要がある旨の情報として、上記2ビットデータ「10」を鍵入手手段302へ送る。鍵入手手段302は、2ビットデータ「10」と送信装置の識別番号とを添えて、暗号鍵の入手を開始するための鍵情報の転送要求をD-IF1394入出力手段102aに送る。尚、送信装置の識別番号は、ソースID906

（図6参照）に格納されているものである。

【0063】尚、転送要求へのコピー管理情報の添付のやり方には、上述した通り、2通りのやり方がある。これに関しては、以下に述べる場合においても同様である。

【0064】送信装置101（図2参照）では、受信装置102からの鍵情報の転送要求を受信する。鍵配布手段206は、上記転送要求の発信元との所定の認証手続きを経た後、鍵発生手段203に対して、転送要求に付されている上記2ビットデータ「10」（コピー管理情報）を送る。この認証手続きとは、相手が正しい機器であるかどうかを判定する為の手続きである。鍵発生手段203は、その「10」に対応する暗号モード（即ち、鍵のグループ）及び、そのグループ内の対応する鍵がどれであるかを調べ、それが鍵のグループA内の鍵A1であると判断した後、その鍵を生成するか、あるいは既に作成して保存されている同じ鍵A1を得るかして、上記転送要求の発信元に対して転送する。尚、この様に、鍵配布手段206が、鍵保存手段204に保存されている暗号鍵A1をそのまま転送せずに、わざわざ、転送要求に付されている上記2ビットデータ「10」（コピー管理情報）を用いて、それに対応する鍵のグループ及び、そのグループ内の暗号鍵を調べることとしたのは、従来の課題の欄で述べた不正行為を防止するためである。これについては、更に後述する。

【0065】一方、受信装置102（図3参照）では、鍵入手手段302が、送信装置101側から転送されてきた暗号鍵A1を得て、鍵保存手段306へ送る。復号

化手段304は鍵保存手段306から得た、暗号鍵A1を用いて、パケット解読手段301からの送られてきた暗号化されたデータを復号し、データ記録再生手段305に送る。

【0066】データ記録再生手段305は、Syフィールド910に格納されているデータ「10」がコピー1回可能であることを判定して、内蔵する記録媒体に、復号化された第2のAVデータを記録しながら、表示手段307、音声出力手段308にも同時に出力する。

【0067】ここで、データ記録再生手段305は、第2のAVデータを記録する場合、Syフィールド910に格納されているコピー管理情報である「10」のデータを「11」と書き換えた上で上記記録動作を行うものである。これは、上記記録によりコピーが1回実行されたことになり、その記録媒体からのその後のコピーは禁止すべきだからである。但し、実データ905の中に含まれているコピー管理情報の書き換えは行わない。尚、第2のAVデータの転送が開始されるT1時刻においては、暗号鍵がその直前に使用していたものとは変化しているので、受信装置102は、上述の様に新たな鍵を入手するまでは、第2のAVデータを復号出来ないという問題を避けるため、第2のAVデータの送信開始からしばらくの間は、暗号化を行わないようにしても勿論良い。ここで、しばらくの間とは、例えば、受信装置102側において、新たな鍵の入手が完了するまでの間である。

【0068】(2)次に、時刻T2～T3における動作を述べる。

【0069】この間は、Syフィールド910にイントランジションモードを示す変更情報「01」が格納されている。受信装置102のパケット解読手段301は、Syフィールド910に2ビットデータ「01」が格納されていることを検出すると、その変更情報「01」を復号化手段304へ送り、鍵の更新がある旨を予告し、復号化手段304は、新たな復号処理の準備を開始する。又、モード検出手段303は、上記2ビットデータ「01」が変更情報であることを検出して、鍵入手手段302に対して、新たな鍵の入手が必要である旨を伝える。ここでも、所定時間後に変更される予定の新たな鍵の転送要求に際し、上述した通り、コピー管理情報が必要となる。しかし、この場合、Syフィールド910には、コピー管理情報は格納されていないので、イントランジションモードの情報が送られてくる直前前に送られてきたコピー管理情報の「10」を使用する。従って、鍵入手手段302は、送信装置101に対して、直前のコピー管理情報の「10」を添えて上記鍵の転送要求を出す。

【0070】尚、鍵のグループが変更されていないので、コピー管理情報の「10」を送らない構成としてもかまわない。

【0071】一方、送信装置101では、鍵配布手段206が上記新たな鍵の転送要求を受けて、切り替えタイミング決定手段207により決定される時刻T3から使用される予定の新たな鍵A2の生成を鍵発生手段203へ要求し、生成された新たな鍵A2を受信装置102側へ転送する。時刻T1においては、受信装置102からの鍵情報の転送要求を受信した送信装置101は、鍵を転送要求の発信元に対して転送する前に上記転送要求の発信元との所定の認証手続きを行っていた。この様に既に認証手続きが終了しているため、今回は(即ち、時刻T2から時刻T3の間では)、鍵の転送前に再度認証手続きを行う必要はない。尚、生成された鍵A2は、鍵保存手段204へも送られる。又、鍵配布手段206は、所定のやりとりの結果、受信装置102への鍵の配布が完了したことを確認して、配布完了情報206aを切り替えタイミング決定手段207へ送る。切り替えタイミング決定手段207は、配布完了情報を得た後、暗号化手段205に対して、それまで使用していた鍵を鍵保存手段204から得た新たな鍵A2に変更して、暗号化を行うことを指示する。これにより、時刻T3からは、暗号鍵A2により暗号化された第2のAVデータ402がデータパケットとして1394バス105上に転送される。

【0072】受信装置102側では、既に新たな鍵A2は入手完了しているので、暗号鍵A2により暗号化された第2のAVデータ402がデータパケットととして受信した場合でも、問題なく復号出来る。その後の動作は、上述した(1)の場合と同様である。

【0073】(3)次に、時刻T4～T5における動作を述べる。

【0074】この場合は、新たな鍵が鍵A3である点を除いて、上記(2)と同様である。

【0075】尚、このように、同一のモード内においても、暗号鍵を時間とともに更新することとしたのは、暗号化の安全性をより一層確保するためである。即ち、同じ鍵の使用時間が長くなるほど、不正行為による暗号の解読のチャンスが増加する。

【0076】一方、同一鍵による暗号化データの蓄積量も大きくなり、仮に、暗号が不正に解読された場合の被害も大きくなることを考慮したものである。

【0077】(4)次に、時刻T6における動作を述べる。

【0078】この場合は、時刻T6においてコピーフリーの音声データ403の転送が開始されるので、暗号鍵は存在しない。従って、時刻T6の直前では、上述の様な予告としての変更情報「01」は出されない。

【0079】受信装置102では、パケット解読手段301が、受信されたデータパケットのSyフィールド910に「00」が格納されていることを検出して、実データ905は暗号化されていないと判定して、実データ

905をデータ記録再生手段305へ直接送る。又、送信装置101に対する鍵の転送要求も行わない。データ記録再生手段305での動作は、上述した内容と同様である。

【0080】(5)次に、時刻T7における動作を述べる。

【0081】この場合、転送対象のデータが第3のAVデータ404であり、これがコピー禁止のデータであることから、上記(1)の場合と動作内容は同じである。尚、本実施の形態では、上述した不正な暗号の解読を防止するという主旨から、同一のコピー管理情報が与えられている転送データにおいて、それぞれが別個独立のものであるか、あるいは、それぞれが時間的に不連続であるかに関わらず、時間とともに暗号鍵を更新するものであり、ここでも、第1のAVデータ401の暗号化に使用した鍵B1から鍵B2に変更している。但し、鍵B1も鍵B2も、鍵のグループは同じグループBに属している。

【0082】ところで、第3のAVデータを受信する場合を例にとり、上述した通り、コピー管理情報を改竄したとしてもそれ以上の不正行為を防止することが出来る点について詳細に述べる。

【0083】即ち、1394バス105上のどこかで不正行為が行われ、受信装置102が受信した第3のAVデータ404において、Syフィールドの「11」情報が「10」に改竄されている場合を考える。

【0084】鍵入手手段302(図3参照)は、上述したとおり、この改竄された「10」のデータを添えて、上記鍵の転送要求を行う。この転送要求を得た、鍵配布手段206(図2参照)は、添えられている「10」を鍵発生手段203へ送り、鍵発生手段203は、「10」に対応する鍵のグループ及び、そのグループ内の暗号鍵を調べ、グループAに属する鍵であると判断して、グループAに属する鍵を生成し、それが受信装置102へ送られる。受信装置102の復号化手段304は、第3のAVデータ404の復号に、グループAに属する鍵を使用しても正しい復号は行えない。本来の鍵は、グループBに属する鍵B2であるからである。

【0085】従って、データ記録再生手段305は、正しく復号されない意味不明の状態のデータをコピー管理情報「10」の内容通り、1回だけ記録媒体に記録するが、このような記録データは全く使用価値が無く、不正行為は無駄な行為となるのである。又、この場合、表示手段307への表示も意味不明の画像となる。尚、正しく復号されなかったデータについては、記録動作を行わない様にデータ記録再生手段305を構成しておいても勿論良い。

【0086】尚、本発明の暗号化の種類は、上記実施の形態では、暗号鍵であったが、これに限らず例えば、暗号のアルゴリズムであっても良い。この場合、送信対象

となるデータの管理情報に応じて上記データの送信に適用する暗号のアルゴリズムを変える構成となる。又、そのアルゴリズムの変え方として具体的には、例えば、大きく分けて次の様な2通りのやり方がある。即ち、一つは、暗号化処理手順の順番を入れ替えることにより、暗号のアルゴリズムを異ならせるものであり、他の一つは、暗号化処理手順のループ回数を変えることにより、暗号のアルゴリズムを異ならせるものである。前者の場合、例えば、所定データに対して、第1の暗号化処理を適用し、その処理結果に対して、更に、第2の暗号化処理を適用した場合の暗号化データと、上記第1と第2の暗号化処理の順番を逆に適用した場合の暗号化データとが異なるという特性を利用するものであり、暗号化回路等のハードウェアの構成を複雑にすることなく実現出来るものである。尚、この場合、双方の暗号化データの暗号の強度は同じレベルである。又、後者の場合、例えば、所定データに対して、第1の暗号化処理を適用し、その結果に対して、更に同じ暗号化処理を適用するという動作の繰り返し回数を一般にループ回数というが、このループ回数を変えることにより、暗号化データを異ならせるというものである。尚、この場合、一般にループ回数を多くしたもののほど暗号の強度が上がる。又、言うまでもなく、前者と後者を組み合わせたものとして、暗号化処理手順の順番を変え、且つ、各暗号化処理のループ回数も変える構成でも良い。更に又、上記の場合、暗号鍵は同一でも良いし、異ならせても良い。以上述べた、暗号のアルゴリズムを変えるという構成を適用する場合、送信装置が、受信装置側に対して送信すべき復号化情報としては、前者の場合は、例えば、暗号化処理の順番であり、後者の場合は、例えば、ループ回数である。

【0087】又、上記実施の形態では、データ記録再生手段が、コピー1回可能とされるデータの記録の際に、Syフィールドに格納されているコピー管理情報を書き換えることについて説明した。ここでは、その点について更に述べる。上記実施の形態でも述べた様に、データ記録再生手段は、実データの中に含まれているコピー管理情報までは書き換えない。そのため、その記録データが、その後、別の記録装置等に送信される場合、Syフィールド内の情報と、実データ内の情報が一致していないため、その別の記録装置において混乱が生じることも考えられる。そこで、本来は、双方の情報は一致させるべきものであるが、装置の構成が複雑になることを避けるため、あえて不一致状態を許し、その代わり、Syフィールドには、その旨を示す情報を書き込む構成としても良い。即ち、コピー1回可能のデータを受信し記録した後、送信する際に、実データ内のコピー管理情報は書き換えていないが、実データのコピーは禁止であることを示す情報として、新たに「ストリームコピー」と名付け、Syフィールドに格納する2ビットデータは「0

1」とするものである。この場合、データ記録再生手段305は、AVデータを記録する場合、Syフィールド910に格納されているコピー管理情報である「10」のデータを、更なるコピー禁止を意味する「01」と書き換えた上で上記記録動作を行う。これにより、正規の装置においては、コピー管理情報としてもともとコピー禁止であるというデータと、1回コピーが実行されたために、その後のコピーが禁止であるというデータの区別が可能となる。従って、Syフィールド内の情報により、混乱無く正しく動作させることが可能となる。更に又、この場合、上記実施の形態で述べたものと同様の構成により、コピー管理情報としての「ストリームコピー」に対応した新たな暗号化の種類（例えば、暗号鍵のグループC）を設けることが出来る。つまり、上述の様に、コピー1回可能のデータが受信され記録された後、その記録データ（第2世代のデータ）を更に送信する装置があった場合、その第2世代のデータのコピー管理情報についても、上記と同様の効果を発揮出来る様にするためである。

【0088】又、この場合、上記実施の形態で述べた、イントランジション情報は、Syフィールドでは、表せないで、例えば、アイソクロノスケットヘッダ900内の、Syフィールド910とは別の領域に独立した1ビットとして確保し、そこに格納する構成としても良い。

【0089】又、上記実施の形態では、イントランジション情報「01」がSYフィールド910に格納される場合について述べたが、これに限らず例えば、アイソクロノスケットヘッダ900内の、Syフィールド910とは別の領域に独立した1ビットを確保し、そこに格納する構成としても良い。

【0090】又、上記実施の形態では、受信装置が、時間とともに変化する鍵の予告情報を受けた後、新たな鍵の転送要求を出す場合について述べた。しかし、これに限らず例えば、送信装置は、上記予告情報の代わりに更新情報を送信し、その更新情報を受信した受信装置から鍵の転送要求が有った場合、上記送信装置が、その転送を要求された鍵に加えて、次に使用する予定の鍵も同時に送るという構成でも良い。ここで、上記更新情報は、鍵の種類（即ち、暗号化の種類）が、上述の様に時間と共に更新される場合に、その更新が実行されたことを受信装置に通知するための情報であり、変更情報発生手段208により生成される（図2参照）。尚、本発明の更新実行情報生成手段は、この変更情報発生手段208に対応する。

【0091】この場合、図5に示すように、独立した1ビットを確保したイントランジション情報が、上記更新情報に対応するものであり、新たな鍵を使用するタイミングを受信装置に知らせることになる。

【0092】即ち、図5において、受信装置は、時刻T

1の直後に鍵A1と鍵A2とを同時に入手しており、時刻T3の時点で、イントランジション情報が、0から1に反転すると、この反転のタイミングを検出した受信装置は、新たな鍵（鍵A2）の使用を開始する。又、この時、受信装置は送信装置に対し、上述した通り、鍵の転送要求を行う。この転送要求に対して、送信装置から現在使用中の鍵A2と、次に使用する予定の鍵A3とが同時に送られてくる。従って、鍵A2については、既に送ったものと重複することになる。そこで、受信装置は、鍵A3についてはこれを保持するが、鍵A2については、既に取得した鍵をそのまま使用し、2度目に送られてきた鍵A2は捨てる。尚、これとは異なり、既に取得した鍵を、2度目に送られてきた鍵A2と差し替えて使用しても勿論良い。

【0093】又、図5において、時刻T5では、1から0に反転するので、この反転を検出した後は、上記と同様の動作となる。上記内容は、勿論、暗号鍵に限らず、例えば、暗号のアルゴリズムを変える場合でも同様に適用出来る。

【0094】また、上記各実施の形態では、説明を簡単にするために復号化情報として鍵をそのまま送信していたが、復号化情報はこれに限るものではなく、受信装置が鍵を作成できる情報であればどのような情報であってもよい。例えば、鍵を暗号化して受信装置に送信し、受信装置は暗号化された鍵を復号化して鍵自身を入手するようにしてもよい。この復号化に必要な情報は認証手続きの際に送信装置と受信装置との間で共有したり、装置製造時に予め送信装置と受信装置に記憶させておいても良い。このようにすれば、鍵の送信を第3者に盗聴されたとしても、第3者には鍵が渡らない。

【0095】又、上記実施の形態では、同一のコピー管理情報のデータについても、暗号化鍵を時間とともに異ならせる場合について述べたが、これに限らず例えば、コピー管理情報に応じて、鍵や暗号化のアルゴリズムを異ならせる構成であれば、時間的に異ならせなくてもかまわない。

【0096】又、上記実施の形態では、コピー管理情報として、コピーフリー、コピー1回可能、コピー禁止などを用いる場合について述べたが、これに限らず例えば、コピー回数の異なるものがあったても勿論良く、これに限るものではない。

【0097】又、以上述べた実施の形態及びそれらの変形例の何れか一つの例に記載の各手段の全部又は一部の手段の機能をコンピュータに実行させるためのプログラムを記録した磁気記録媒体や光記録媒体などの記録媒体を作成し、それを利用することにより上記と同様の動作を実行させることが出来る。

【0098】又、上記実施の形態及びそれらの変形例の各手段の処理動作は、コンピュータを用いてプログラムの働きにより、ソフトウェア的に実現してもよいし、あ

るいは、上記処理動作をコンピュータを使用せずに特有の回路構成により、ハードウェア的に実現してもよい。

【0099】

【発明の効果】以上述べたところから明らかなように本発明は、伝送データの保護が従来に比べてより一層確実に行えるという長所を有する。

【図面の簡単な説明】

【図1】本発明の実施の形態におけるデータ伝送システムの概略構成図

【図2】同実施の形態における送信装置の構成を示すブロック図

【図3】同実施の形態における受信装置の構成を示すブロック図

【図4】同実施の形態における、暗号鍵の時刻による変化を示す説明図

【図5】本発明の別の実施の形態における、暗号鍵の時刻による変化を示す説明図

【図6】従来のデータ転送方法におけるアイソクロノスパケットのフォーマットを表す説明図

【符号の説明】

101 送信装置

101a

102a

102~104

105

202

203

206

207

種類更新手段)

208

段)

301

出手段)

302

303

304

305

段)

401

1394入出力手段(データ送信手段)

1394入出力手段(データ受信手段)

受信装置

IEEE1394バス

モード決定手段

鍵発生手段(暗号化種類更新手段)

鍵配布手段(復号化情報送信手段)

切り替えタイミング決定手段(暗号化

変更情報発生手段(予告情報生成手

ケット解読手段(データ管理情報検

鍵入手手段(復号化情報要求手段)

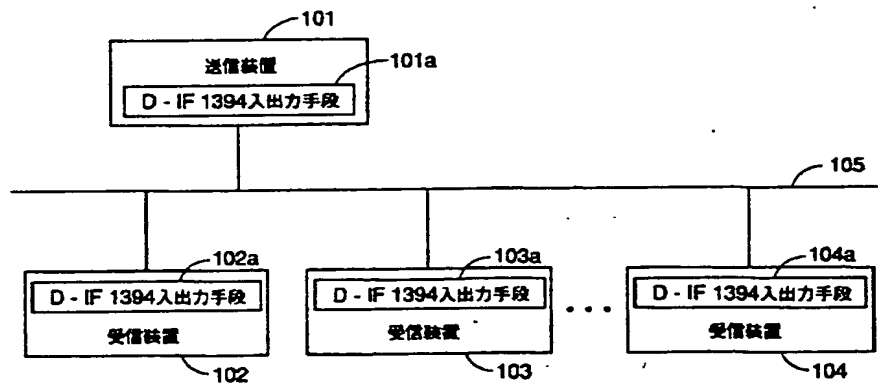
モード検出手段

復号化手段

データ記録再生手段(処理方法決定手

第1のAVデータ

【図1】



送信装置

101

105

101a

D-IF 1394

202

モード決定手段

203

発生手段

204

発生手段

205

ラッチ
暗号化手段

206

配布手段

206b

配布完了

207

切替えタイミング
決定手段

207a

切替え情報

208

変更情報
発生手段

208a

209

パケット
生成手段

データ 201 a

データ 205a

データパケット 209a
(間期)

(非同期)

The diagram illustrates the internal structure of a receiving device (102). The components and their interconnections are as follows:

- 102a D-IF 1394**: The primary interface for receiving data.
- 301 パケット解析手段** (Packet Analysis Unit): Receives data from 102a and outputs **データバケット209a (同期)** (Data Bucket 209a, Synchronous) to 304. It also outputs **変更情報 310** (Change Information 310) to 305.
- 302 搬入手段** (Loading Unit): Receives data from 102a and outputs **搬送 203a (非同期)** (Transport 203a, Asynchronous) to 303.
- 303 モード検出手段** (Mode Detection Unit): Receives transport data from 302 and outputs **実データ 905** (Actual Data 905) to 304.
- 304 復号化手段** (Decoding Unit): Receives **実データ 905** from 303 and outputs it to 307. It also receives **データバケット209a (同期)** from 301.
- 305 データ記録再生手段** (Data Recording/Reproduction Unit): Receives **変更情報 310** from 301 and outputs **実データ 905** to 304. It also receives **データバケット209a (同期)** from 301.
- 306 搬送手段** (Transport Unit): Receives **実データ 905** from 304 and outputs it to 302.
- 307 表示手段** (Display Unit): Receives **実データ 905** from 304.
- 308 音声出力手段** (Audio Output Unit): Receives **実データ 905** from 304.

時刻

T1 T2 T3 T4 T5 T6 T7

Syフィールド内のデータ: 11 10 01 10 01 10 00 11

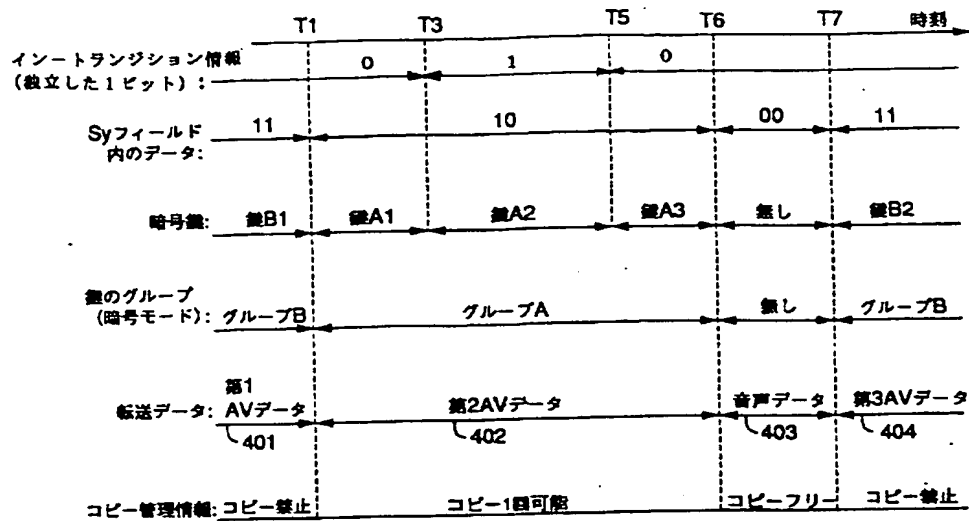
暗号鍵: 鍵B1 鍵A1 鍵A2 鍵A3 無し 鍵B2

鍵のグループ (暗号モード): グループB グループA 無し グループB

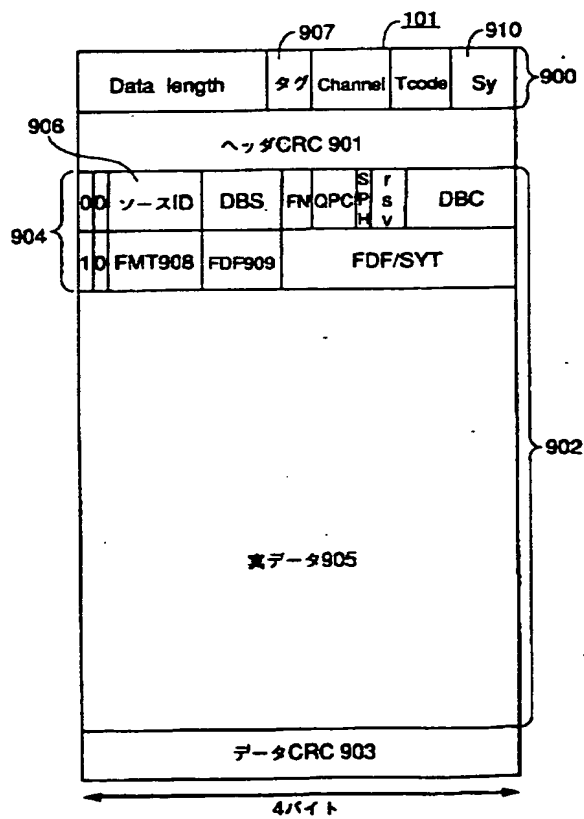
転送データ: 第1 AVデータ (401) 第2AVデータ (402) 音声データ (403) 第3AVデータ (404)

コピー管理情報: コピー禁止 コピー1回可能 コピーフリー コピー禁止

【図5】



【図6】



フロントページの続き

(72)発明者 松崎 なつめ
大阪府門真市大字門真1006番地 松下電器
産業株式会社内